

Conteúdo

prefácio xv

agradecimentos xx

sobre este livro xxi

sobre o autor xxvi

sobre a ilustração da capa xxvii

PARTE 1 — PRIMITIVAS: OS INGREDIENTES

DA CRIPTOGRAFIA 1

1 Introdução 3

1.1 Criptografia trata de proteger protocolos 4

1.2 Criptografia simétrica: O que é criptografia simétrica? 5

1.3 Princípio de Kerckhoff: Apenas a chave é mantida em segredo 7

1.4 Criptografia assimétrica: Duas chaves são melhores do que uma 10

Trocas de chaves ou como obter um segredo compartilhado 10 ■

Criptografia assimétrica, diferente da simétrica 13 ■

Assinaturas digitais, assim como suas assinaturas à caneta e papel 15

1.5 Classificando e abstraindo a criptografia 17

1.6 Criptografia teórica vs. criptografia do mundo real 18

1.7 Do teórico ao prático: Escolha sua própria aventura 19

1.8 Uma palavra de advertência 24

2 Funções de hash 25

2.1 O que é uma função de hash? 25

2.2 Propriedades de segurança de uma função de hash 28

2.3 Considerações de segurança para funções de hash 30

2.4 Funções de hash na prática 31

Comprometimentos 32 ■ Integridade de subrecursos 32

BitTorrent 32 ■ Tor 33

2.5 Funções de hash padronizadas 34

A função de hash SHA-2 35 ■ A função de hash SHA-3 38

SHAKE e cSHAKE: Duas funções de saída extensível (XOF) 42

Evite hash ambíguo com TupleHash 43

2.6 Hasheando senhas 44

3 Códigos de autenticação de mensagens (MACs) 48

3.1 Cookies sem estado, um exemplo motivador para MACs 48

3.2 Um exemplo em código 51

3.3 Propriedades de segurança de um MAC 52

Falsificação de tag de autenticação 53 ■ Comprimentos de tags de autenticação 53 ■ Ataques de repetição 54 ■ Verificando tags de autenticação em tempo constante 55

3.4 MACs no mundo real 57

Autenticação de mensagens 57 ■ Derivação de chaves 57 ■ Integridade de cookies 58 ■ Tabelas de hash 58

3.5 MACs na prática 58

HMAC, um MAC baseado em hash 58 ■ KMAC, um MAC baseado em cSHAKE 59

3.6 SHA-2 e ataques de extensão de comprimento 60

4 Criptografia autenticada 64

4.1 O que é um cifrador? 65

4.2 O cifrador em bloco AES (Padrão de Criptografia Avançada) 66

Quanto de segurança o AES oferece? 67 ■ A interface do AES 67 ■ Os internos do AES 68

4.3 O pinguim criptografado e o modo de operação CBC 70

4.4 Falta de autenticidade, portanto AES-CBC-HMAC 73

4.5 Construções tudo-em-um: Criptografia autenticada 74

O que é criptografia autenticada com dados associados (AEAD)? 75

O AEAD AES-GCM 76 ■ ChaCha20-Poly1305 81

4.6 Outros tipos de criptografia simétrica 84

Empacotamento de chaves 84 ■ Criptografia autenticada resistente ao mau uso de nonce 85 ■ Criptografia de disco

85 ■ Criptografia de banco de dados 85

5 Trocas de chaves 87

5.1 O que são trocas de chaves? 88

5.2 A troca de chaves de Diffie-Hellman (DH) 91

Teoria dos grupos 91 ■ O problema do logaritmo discreto: A base do Diffie-Hellman 95 ■ Os padrões de Diffie-Hellman 97

5.3 A troca de chaves Elliptic Curve Diffie-Hellman (ECDH) 98

O que é uma curva elíptica? 98 ■ Como funciona a troca de chaves ECDH? 102 ■ Os padrões para ECDH 103

5.4 Ataques de subgrupos pequenos e outras considerações de segurança 105

6 Criptografia assimétrica e criptografia híbrida 109

6.1 O que é criptografia assimétrica? 110

6.2 Criptografia assimétrica na prática e criptografia híbrida 111

Trocas de chaves e encapsulamento de chaves 112 ■ Criptografia híbrida 113

6.3 Criptografia assimétrica com RSA: O ruim e o menos ruim 117

RSA direto (textbook RSA) 117 ■ Por que não usar RSA PKCS#1 v1.5 121

Criptografia assimétrica com RSA-OAEP 123

6.4 Criptografia híbrida com ECIES 126

7 Assinaturas e provas de conhecimento zero 129

7.1 O que é uma assinatura? 130

Como assinar e verificar assinaturas na prática 131 ■ Um caso de uso primário: Trocas de chaves autenticadas 132 ■ Um uso no mundo real: Infraestruturas de chaves públicas 133

7.2 Provas de conhecimento zero (ZKPs): A origem das assinaturas 134

Protocolo de identificação de Schnorr: Uma prova interativa de conhecimento zero 134 ■ Assinaturas como provas não interativas de conhecimento zero 137

7.3 Os algoritmos de assinatura que você deve (ou não) usar 138

RSA PKCS#1 v1.5: Um padrão ruim 139 ■ RSA-PSS: Um padrão melhor 142 ■ Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA) 143 ■ Algoritmo de Assinatura Digital de Curva Edwards (EdDSA) 145

7.4 Comportamentos sutis de esquemas de assinatura 149

Ataques de substituição em assinaturas 149 ■ Maleabilidade de assinatura 150

8 Aleatoriedade e segredos 152

8.1 O que é aleatoriedade? 153

8.2 Aleatoriedade lenta? Use um gerador de números pseudoaleatórios (PRNG) 155

8.3 Obtendo aleatoriedade na prática 158

8.4 Geração de aleatoriedade e considerações de segurança 161

8.5 Aleatoriedade pública 163

8.6 Derivação de chaves com HKDF 164

8.7 Gerenciando chaves e segredos 168

8.8 Descentralizando confiança com criptografia com limiar 169

PARTE 2 — PROTOCOLOS: AS RECEITAS

DA CRIPTOGRAFIA 175

9 Transporte seguro 177

9.1 Os protocolos de transporte seguro SSL e TLS 177

Do SSL ao TLS 178 ■ Usando TLS na prática 179

9.2 Como funciona o protocolo TLS? 181

O handshake TLS 181 ■ Como o TLS 1.3 criptografa dados de aplicação 194

9.3 O estado da web criptografada hoje 194

9.4 Outros protocolos de transporte seguro 197

9.5 O framework de protocolo Noise: Uma alternativa moderna ao TLS 197

Os muitos handshakes do Noise 198 ■ Um handshake com Noise 199

10 Criptografia de ponta a ponta 201

10.1 Por que criptografia de ponta a ponta? 202

10.2 Nenhuma raiz de confiança a ser encontrada 203

10.3 O fracasso do e-mail criptografado 205

PGP ou GPG? E como funciona? 205 ■ Escalando a confiança entre usuários com a teia de confiança 208 ■ Descoberta de chaves é um problema real 208 ■ Se não for PGP, então o quê? 210

10.4 Mensageria segura: Uma visão moderna com o Signal 211

Mais amigável que a WOT: Confiança mas verificação 212 ■ X3DH: O handshake do protocolo Signal 215 ■ Double Ratchet: O protocolo pós-handshake do Signal 218

10.5 O estado da criptografia de ponta a ponta 222

11 Autenticação de usuários 226

11.1 Um resumo da autenticação 227

11.2 Autenticação de usuários, ou a busca por eliminar senhas 228

Uma senha para governar todas: Single sign-on (SSO) e gerenciadores de senha 231 ■

Não quer ver as senhas deles? Use uma troca de chaves autenticada por senha assimétrica 232 ■

Senhas únicas não são realmente senhas: Indo sem senha com chaves simétricas 236 ■ Substituindo senhas por chaves assimétricas 239

11.3 Autenticação assistida por usuários: Pareando dispositivos com ajuda humana 242

Chaves pré-compartilhadas 244 ■ Trocas de chaves autenticadas por senha simétrica com CPace 245 ■ Meu key exchange sofreu MITM? Verifique uma cadeia autenticada curta (SAS) 246

12 Cripto como em criptomoeda? 251

12.1 Uma introdução suave aos algoritmos de consenso tolerantes a falhas bizantinas (BFT) 252

Um problema de resiliência: Protocolos distribuídos ao resgate 252

Um problema de confiança? A descentralização ajuda 254 ■ Um problema de escala: Redes permissionless e resistentes à censura 255

12.2 Como o Bitcoin funciona? 257

Como o Bitcoin gerencia saldos e transações dos usuários 257

Minerando BTCs na era digital do ouro 259 ■ Inferno dos forks! Resolvendo conflitos na mineração 263 ■ Reduzindo o tamanho do bloco com árvores de Merkle 265

12.3 Um passeio pelas criptomoedas 267

Volatilidade 267 ■ Latência 267 ■ Tamanho do blockchain 268 ■ Confidencialidade 268 ■ Eficiência energética 268

12.4 DiemBFT: Um protocolo de consenso BFT 269

Segurança e vivacidade: As duas propriedades de um protocolo BFT 269 ■

Uma rodada no protocolo DiemBFT 270 ■ Quanto desonestidade o protocolo tolera? 270 ■

As regras de votação do DiemBFT 271 ■ Quando as transações são consideradas finalizadas? 273 ■

Intuições por trás da segurança do DiemBFT 273

13 Criptografia em hardware 277

13.1 Modelo de atacantes da criptografia moderna 278

13.2 Ambientes não confiáveis: Hardware ao resgate 279

Criptografia white-box, uma má ideia 280 ■ Estão na sua carteira: Smart cards e elementos seguros 281 ■

Bancos adoram: Módulos de segurança de hardware (HSMs) 283 ■

Trusted Platform Modules (TPMs): Uma padronização útil de elementos seguros 285 ■

Computação confidencial com ambientes de execução confiáveis (TEEs) 288

13.3 Qual solução é boa para mim? 289

13.4 Criptografia resistente a vazamentos ou como mitigar ataques de canal lateral em software 291

Programação em tempo constante 293 ■ Não use o segredo! Mascaramento e blindagem 294 ■

E quanto a ataques por falha? 295

14 Criptografia pós-quântica 298

14.1 O que são computadores quânticos e por que assustam os criptógrafos? 299

Mecânica quântica, o estudo do pequeno 299 ■ Do nascimento dos computadores quânticos à supremacia quântica 302 ■

O impacto dos algoritmos de Grover e Shor na criptografia 303 ■

Criptografia pós-quântica, a defesa contra computadores quânticos 304

14.2 Assinaturas baseadas em hash: Só precisa de uma função de hash 305

Assinaturas de uso único com assinaturas de Lamport 305 ■ Chaves menores com assinaturas Winternitz 307 ■ Assinaturas de múltiplos usos com XMSS e SPHINCS+ 308

14.3 Chaves e assinaturas menores com criptografia baseada em reticulados 311

O que é um reticulado? 311 ■ Aprendizado com erros (LWE), uma base para a criptografia? 313 ■

Kyber, uma troca de chaves baseada em reticulados 314 ■ Dilithium, um esquema de assinatura baseado em reticulados 316

14.4 Eu preciso entrar em pânico? 318

15 É isso? Criptografia de próxima geração 321

15.1 Quanto mais, melhor: Computação multipartidária segura (MPC) 322

Interseção de conjuntos privados (PSI) 323 ■ MPC de propósito geral 324 ■ O estado do MPC 326

15.2 Criptografia homomórfica totalmente funcional (FHE) e as promessas de uma nuvem criptografada 326

Um exemplo com RSA 327 ■ Os diferentes tipos de FHE 327 ■ Bootstrapping: a chave para o FHE 328 ■

Um esquema de FHE baseado em LWE 330 ■ Onde está sendo usado? 332

15.3 Provas de conhecimento zero de propósito geral (ZKPs) 332

Como funcionam zk-SNARKs 335 ■ Comprometimentos homomórficos para esconder partes da prova 336 ■ Pareamentos bilineares para melhorar os comprometimentos 336 ■

De onde vem a sucintez? 337 ■ De programas a polinômios 338 ■ Circuitos aritméticos e sistemas de restrição rank-1 (R1CS) 339 ■

De R1CS a um polinômio 340 ■ São necessárias duas partes para avaliar um polinômio oculto no expoente 340

16 Quando e onde a criptografia falha 343

16.1 Encontrar a primitiva ou protocolo certo é um trabalho tedioso 344

16.2 Como usar primitivas ou protocolos criptográficos? Padrões educados e verificação formal 345

16.3 Onde estão as boas bibliotecas? 348

16.4 Uso indevido da criptografia: os desenvolvedores são o inimigo 349

16.5 Você está fazendo errado: segurança utilizável 351

16.6 A criptografia não é uma ilha 352

16.7 Suas responsabilidades como praticante de criptografia: não invente sua própria criptografia 353

Apêndice — Respostas dos exercícios 357

Índice 361

Prefácio

Como você pegou este livro, pode estar se perguntando: por que mais um livro sobre criptografia? Ou até mesmo, por que eu deveria ler este livro? Para responder a isso, você precisa entender quando tudo começou.

Um livro, anos em formação

Hoje em dia, se você quer aprender sobre quase qualquer coisa, você procura no Google, ou Bing, ou Baidu — você entendeu. No entanto, para criptografia, e dependendo do que você está procurando, os recursos podem ser bastante escassos. Isso foi algo que enfrentei há muito tempo e que tem sido uma fonte contínua de frustração desde então.

Na época em que eu estava na escola, tive que implementar um ataque de análise de potência diferencial para uma aula. Esse ataque foi um avanço na criptoanálise naquela época, sendo o primeiro ataque de canal lateral publicado. Um ataque de análise de potência diferencial é algo mágico: ao medir o consumo de energia de um dispositivo enquanto ele criptografa ou descriptografa algo, você consegue extrair seus segredos. Eu percebi que artigos excelentes podiam transmitir grandes ideias, mas com pouco esforço em clareza e inteligibilidade. Lembro de bater a cabeça na parede tentando entender o que o autor queria dizer. Pior, eu não conseguia encontrar bons recursos online que explicassem o artigo. Então bati a cabeça mais um pouco e finalmente entendi. E então pensei, talvez eu pudesse ajudar outros como eu que teriam que passar por essa provação.

Motivado, desenhei alguns diagramas, os animei e gravei a mim mesmo explicando-os. Esse foi meu primeiro vídeo no YouTube sobre criptografia:

<https://www.youtube.com/watch?v=gbqNCgVcXsM>

Anos depois, ainda recebo elogios de pessoas aleatórias na internet. Ontem mesmo, enquanto escrevo este prefácio, alguém comentou: "Obrigado, realmente uma explicação ótima que provavelmente me salvou horas tentando entender aquele artigo."

Que recompensa! Esse pequeno passo em me aventurar no outro lado da paisagem educacional foi suficiente para me fazer querer fazer mais. Comecei a gravar mais desses vídeos e, em seguida, iniciei um blog para escrever sobre criptografia. Você pode conferir aqui: <https://cryptologie.net>

Antes de começar este livro, eu já havia acumulado quase 500 artigos explicando os muitos conceitos além desta introdução. Tudo isso era apenas prática. No fundo da minha mente, a ideia de escrever um livro vinha amadurecendo anos antes de a Manning Publications entrar em contato comigo com uma proposta.

O currículo do criptógrafo do mundo real

Terminei minha graduação em matemática teórica e não sabia o que fazer a seguir. Eu também programava desde sempre e queria reconciliar as duas coisas. Naturalmente, fiquei curioso sobre criptografia, que parecia reunir o melhor dos dois mundos, e comecei a ler os livros disponíveis. Rapidamente descobri minha vocação.

Mas havia algumas coisas irritantes: especialmente as introduções longas que começavam com história; eu estava interessado apenas nos aspectos técnicos e sempre fui assim. Jurei para mim mesmo: se algum dia eu escrevesse um livro sobre criptografia, não escreveria uma única linha sobre cifras de Vigenère, cifras de César e outros vestígios da história. E assim, depois de obter um mestrado em criptografia na Universidade de Bordeaux, achei que estava pronto para o mundo real. Mal sabia eu...

Acreditei que meu diploma era suficiente, mas minha educação carecia muito dos protocolos do mundo real que eu estava prestes a analisar. Passei muito tempo aprendendo sobre a matemática das curvas elípticas, mas nada sobre como elas eram usadas em algoritmos criptográficos. Aprendi sobre LFSRs, ElGamal, DES e uma série de outras primitivas criptográficas que nunca mais veria novamente.

Quando comecei a trabalhar na indústria, na Matasano, que depois se tornou NCC Group, meu primeiro trabalho foi auditar o OpenSSL, a implementação SSL/TLS mais popular — o código que basicamente criptografava toda a internet. Oh, como aquilo doía minha cabeça. Lembro de voltar para casa todo dia com uma forte dor de cabeça. Que bagunça de biblioteca e protocolo! Eu não sabia na época que, anos depois, me tornaria coautor do TLS 1.3, a versão mais recente do protocolo.

Mas, naquele ponto, já estava pensando: "É isso que eu deveria ter aprendido na faculdade. Este conhecimento que estou adquirindo agora é o que teria sido útil para me preparar para o mundo real!" Afinal, eu era agora um especialista em segurança especializado em criptografia. Eu revisava aplicações criptográficas do mundo real. Eu fazia o trabalho que qualquer um desejaria após terminar um curso de criptografia. Eu implementava, verificava, usava e aconselhava quais algoritmos criptográficos usar. É por isso que sou o primeiro leitor do livro que estou escrevendo. Este é o livro que eu teria escrito para meu eu do passado para prepará-lo para o mundo real.

Onde estão a maioria dos erros

Meu trabalho como consultor me levou a auditar muitas aplicações criptográficas do mundo real, como o OpenSSL, o sistema de backup criptografado do Google, a implementação do TLS 1.3 da Cloudflare, o protocolo da autoridade certificadora da Let's Encrypt, o protocolo sapling da criptomoeda Zcash, o esquema de recriptografia por procuração com limiar da NuCypher, e dezenas de outras aplicações criptográficas do mundo real que, infelizmente, não posso mencionar publicamente.

Logo no início do trabalho, fui encarregado de auditar o protocolo personalizado que uma corporação famosa havia escrito para criptografar suas comunicações. Acontece que ele usava assinaturas em quase tudo, exceto nas chaves efêmeras, o que quebrava completamente o protocolo, já que alguém poderia facilmente substituí-las — um erro básico para qualquer um com alguma experiência com protocolos de transporte seguros, mas algo que foi negligenciado por pessoas que pensavam ter experiência suficiente para criar sua própria criptografia. Lembro de explicar a vulnerabilidade no final do trabalho e de ver uma sala cheia de engenheiros ficar em silêncio por bons 30 segundos.

Essa história se repetiu muitas vezes durante minha carreira. Houve uma vez em que, ao auditar uma criptomoeda para outro cliente, encontrei uma maneira de forjar transações a partir de transações já existentes, devido a uma ambiguidade sobre o que estava sendo assinado. Ao olhar implementações de TLS para outro cliente, encontrei maneiras sutis de quebrar uma implementação de RSA, o que, por sua vez, se transformou em um artigo técnico com um dos inventores do RSA, levando a diversos relatórios de CVEs (Common Vulnerabilities and Exposures) para dúzias de projetos de código aberto. Mais recentemente, ao estudar o novo protocolo de chat Matrix enquanto escrevia este livro, percebi que seu protocolo de autenticação estava quebrado, o que levava à quebra de sua criptografia de ponta a ponta. Há tantos detalhes que, infelizmente, podem ruir quando se utiliza criptografia. Nesse ponto, eu sabia que precisava escrever algo sobre isso. Por isso, meu livro contém muitas dessas anedotas.

Como parte do trabalho, eu revisava bibliotecas e aplicações criptográficas em uma infinidade de linguagens de programação. Descobri bugs (por exemplo, o CVE-2016-3959 na biblioteca padrão do Golang), pesquisei maneiras pelas quais bibliotecas poderiam induzir ao uso incorreto (por exemplo, meu artigo “How to Backdoor Diffie-Hellman”), e aconselhei sobre quais bibliotecas usar. Os desenvolvedores nunca sabiam qual biblioteca usar, e eu sempre achava a resposta complicada.

Acabei por inventar o protocolo Disco (<https://discocrypto.com>; <https://embeddeddisco.com>) e escrevi sua biblioteca criptográfica completa em menos de 1.000 linhas de código — e isso, em várias linguagens. Disco se baseava apenas em duas primitivas criptográficas: a permutação do SHA-3 e a Curve25519. Sim, com apenas essas duas coisas implementadas em 1.000 linhas de código, um desenvolvedor poderia realizar qualquer tipo de troca de chaves autenticada, assinaturas, criptografia, MACs, hashing, derivação de chaves e assim por diante. Isso me deu uma perspectiva única sobre o que uma boa biblioteca de criptografia deveria ser.

Quis que meu livro contivesse esses tipos de insights práticos. Assim, naturalmente, os diferentes capítulos contêm exemplos de como aplicar “criptografia” em diferentes linguagens de programação, usando bibliotecas criptográficas bem respeitadas.

A necessidade de um novo livro?

Enquanto eu ministrava uma das minhas sessões anuais de treinamento em criptografia na Black Hat (uma conhecida conferência de segurança), um aluno veio até mim e perguntou se eu poderia recomendar um bom livro ou curso online sobre criptografia. Lembro de ter aconselhado o aluno a ler um livro de Boneh e Shoup e assistir ao curso *Cryptography I* de Boneh no Coursera. (Eu também recomendo ambos os recursos ao final deste livro.)

O aluno me disse: “Ah, eu tentei, mas é muito teórico!” Essa resposta ficou comigo. Discordei a princípio, mas aos poucos percebi que ele estava certo. A maioria dos recursos são bastante pesados em matemática, e a maioria dos desenvolvedores que lidam com criptografia não quer lidar com matemática. O que mais havia para eles?

Os outros dois recursos um tanto respeitadas na época eram *Applied Cryptography* e *Cryptography Engineering* (ambos livros de Bruce Schneier). Mas esses livros estavam começando a ficar bastante desatualizados. *Applied Cryptography* dedica quatro capítulos a cifras de bloco, com um capítulo inteiro sobre modos de operação de cifra, mas nenhum sobre criptografia autenticada. O mais recente *Cryptography Engineering* fazia uma única menção à criptografia de curva elíptica em uma nota de rodapé. Por outro lado, muitos dos meus vídeos ou posts de blog estavam se tornando boas referências primárias para alguns conceitos criptográficos. Eu sabia que poderia fazer algo especial.

Gradualmente, muitos dos meus alunos começaram a se interessar por criptomoedas, fazendo cada vez mais perguntas sobre o assunto. Ao mesmo tempo, comecei a auditar mais e mais aplicações de criptomoeda. Mais tarde, fui trabalhar no Facebook liderando a segurança da criptomoeda Libra (agora conhecida como Diem). Criptomoedas eram, na época, um dos campos mais quentes para se trabalhar, misturando uma multiplicidade de primitivas criptográficas extremamente interessantes que até então tinham visto pouco ou nenhum uso no mundo real (provas de conhecimento zero, assinaturas agregadas, criptografia com limiar, computações multipartidárias, protocolos de consenso, acumuladores criptográficos, funções aleatórias verificáveis, funções de atraso verificáveis, ... a lista continua). E ainda assim, nenhum livro de criptografia incluía um capítulo sobre criptomoedas. Eu estava agora em uma posição única.

Sabia que podia escrever algo que mostrasse a estudantes, desenvolvedores, consultores, engenheiros de segurança e outros o que era a criptografia aplicada moderna. Este seria um livro com poucas fórmulas, mas repleto de diagramas. Um livro com pouca história, mas cheio de histórias modernas sobre falhas criptográficas que eu testemunhei de verdade. Um livro com pouco sobre algoritmos legados, mas repleto de criptografia que eu pessoalmente vi sendo usada em larga escala: TLS, o framework de protocolo Noise, o protocolo Signal, criptomoedas, HSMS, criptografia com limiar e assim por diante. Um livro com pouca criptografia teórica, mas cheio do que pode vir a ser relevante: trocas de chaves autenticadas por senha, provas de conhecimento zero, criptografia pós-quântica, e por aí vai.

Quando a Manning Publications entrou em contato comigo em 2018, perguntando se eu queria escrever um livro sobre criptografia, eu já sabia a resposta. Eu já sabia o que queria escrever. Só estava esperando alguém me dar a

oportunidade e o pretexto para dedicar meu tempo escrevendo o livro que tinha em mente. Coincidentemente, a Manning tem uma série de livros “do mundo real”, então naturalmente sugeri que meu livro a expandisse. O que você tem diante de si é o resultado de mais de dois anos de muito trabalho e muito amor. Espero que goste.

Agradecimentos

Obrigado a Marina Michaels por sua ajuda contínua e insights, sem os quais este livro provavelmente não teria sido concluído.

Obrigado a Frances Buran, Sam Zaydel, Michael Rosenberg, Pascal Knecht, Seth David Schoen, Eyal Ronen, Saralynn Chick, Robert Seacord, Eloi Manuel, Rob Wood, Hunter Monk, Jean-Christophe Forest, Liviu Bartha, Mattia Reggiani, Olivier Guerra, Andrey Labunov, Carl Littke, Yan Ivnitskiy, Keller Fuchs, Roman Zabicki, M K Saravanan, Sarah Zennou, Daniel Bourdreux, Jason Noll, Ilias Cherkaoui, Felipe De Lima, Raul Siles, Matteo Bocchi, John Woods, Kostas Chalkias, Yolan Romailer, Gerardo Di Giacomo, Gregory Nazario, Rob Stubbs, Ján Jančár, Gabe Pike, Kiran Tummala, Stephen Singam, Jeremy O’Donoghue, Jeremy Boone, Thomas Duboucher, Charles Guillemet, Ryan Sleevi, Lionel Rivière, Benjamin Larsen, Gabriel Giono, Daan Sprengels, Andreas Krogen, Vadim Lyubashevsky, Samuel Neves, Steven (Dongze) Yue, Tony Patti, Graham Steel, e a todos os comentaristas do livebook pelas muitas discussões e correções, bem como feedbacks técnicos e editoriais.

A todos os revisores: Adhir Ramjiawan, Al Pezewski, Al Rahimi, Alessandro Campeis, Bobby Lin, Chad Davis, David T Kerns, Domingo Salazar, Eddy Vluggen, Gábor László Hajba, Geert Van Laethem, Grzegorz Bernaś, Harald Kuhn, Hugo Durana, Jan Pieter Herweijer, Jeff Smith, Jim Karabatsos, Joel Kotarski, John Paraskevopoulos, Matt Van Winkle, Michal Rutka, Paul Grebenc, Richard Lebel, Ruslan Shevchenko, Sanjeev Jaiswal, Shawn P Bolan, Thomas Doylend, William Rudenmalm — suas sugestões ajudaram a tornar este um livro melhor.

Sobre este livro

Já se passaram mais de dois anos desde que comecei a escrever *Real-World Cryptography*. Eu originalmente pretendia que fosse uma introdução a tudo o que há para saber sobre o tipo de criptografia que é usada no mundo real. Mas, é claro, essa é uma tarefa impossível. Nenhuma área pode ser resumida em um único livro. Por esse motivo, tive que encontrar um equilíbrio entre a quantidade de detalhes que eu queria oferecer ao leitor e a quantidade de tópicos que eu queria cobrir. Espero que você se encontre na mesma “caixa” em que eu acabei me colocando. Se você está procurando um livro prático que ensine a criptografia que empresas e produtos implementam e usam, e se você é curioso sobre como a criptografia do mundo real funciona por baixo dos panos, mas não está procurando um livro de referência com todos os detalhes de implementação, então este livro é para você.

Quem deve ler este livro

Aqui está uma lista do que acredito serem os tipos de pessoas (embora por favor, não deixe ninguém colocá-lo em uma caixa) que se beneficiariam deste livro.

Estudantes

Se você está estudando ciência da computação, segurança ou criptografia e quer aprender sobre a criptografia tal como é usada no mundo real (porque está mirando um emprego na indústria ou deseja trabalhar em assuntos aplicados na academia), então acredito que este seja o livro-texto para você. Por quê? Porque, como disse no prefácio, eu já fui um desses estudantes, e escrevi o livro que gostaria de ter tido então.

Profissionais de segurança

Pentesters, consultores de segurança, engenheiros de segurança, arquitetos de segurança e outros papéis relacionados compuseram a maioria dos alunos que tive quando lecionei criptografia aplicada. Por causa disso, este

material foi refinado pelas muitas perguntas que recebi enquanto tentava explicar conceitos criptográficos complicados para não-criptógrafos. Como eu também sou um profissional de segurança, este livro também é moldado pela criptografia que auditei para grandes empresas e pelos bugs que aprendi ou descobri ao longo do caminho.

Desenvolvedores que usam criptografia direta ou indiretamente

Este trabalho também foi moldado pelas muitas conversas que tive com clientes e colegas de trabalho, que em sua maioria não eram profissionais de segurança nem criptógrafos. Hoje em dia, está se tornando cada vez mais difícil escrever código sem tocar em criptografia e, como tal, você precisa ter algum entendimento do que está usando. Este livro fornece esse entendimento, com exemplos de código em diferentes linguagens de programação — e mais, se você for curioso.

Criptógrafos curiosos sobre outras áreas

Este livro é uma introdução à criptografia aplicada que é útil para pessoas como eu. Eu escrevi isso, primeiro, para mim mesmo, lembre-se. Se eu conseguir fazer um bom trabalho, um criptógrafo teórico deve ser capaz de obter rapidamente uma compreensão de como é o mundo da criptografia aplicada; outro, que trabalha com criptografia simétrica, deve conseguir entender rapidamente trocas de chaves autenticadas por senha lendo o capítulo correspondente; um terceiro, que trabalha com protocolos, deve conseguir adquirir rapidamente uma boa compreensão de criptografia quântica — e assim por diante.

Gerentes de engenharia e produto que querem entender mais

Este livro também tenta responder a perguntas que considero mais orientadas a produto: quais são as concessões e limitações dessas abordagens? Que risco estou assumindo? Este caminho me ajudaria a cumprir regulações? Preciso fazer isso e aquilo para trabalhar com um governo?

Pessoas curiosas que querem saber do que se trata a criptografia do mundo real

Você não precisa ser nenhum dos tipos listados anteriormente para ler este livro. Você só precisa ser curioso sobre a criptografia como usada no mundo real. Tenha em mente que eu não ensino a história da criptografia, e não ensino o básico da ciência da computação, então, no mínimo, você deveria ter ouvido falar de criptografia antes de começar um livro como este.

Conhecimento prévio presumido — a versão longa

O que você vai precisar para tirar o máximo proveito deste livro? Você deve saber que este livro assume que você tem algum entendimento básico de como seu laptop ou a internet funciona, e, pelo menos, deveria já ter ouvido falar de criptografia. O livro trata de criptografia do mundo real, e por isso será difícil colocar as coisas em contexto se você não se sentir à vontade com computadores ou se nunca ouviu a palavra “criptografia” antes.

Assumindo que você sabe mais ou menos no que está se metendo, será uma vantagem se você souber o que são bits e bytes, e se já viu ou até usou operações bit a bit como XOR, deslocamento à esquerda, e essas coisas. Isso é essencial? Não. Mas pode significar que você terá que parar de vez em quando para fazer algumas buscas antes de continuar a leitura.

Na verdade, não importa o quão qualificado você seja, ao ler este livro, provavelmente vai ter que parar de tempos em tempos para buscar mais informações na internet. Seja porque eu (vergonha!) esqueci de definir um termo antes de usá-lo, ou porque presumi erroneamente que você o conhecia. De todo modo, isso não deve ser um grande problema, pois tento explicar como se você tivesse 5 anos (EL5) da melhor forma possível os diferentes conceitos que introduzo.

Por fim, quando uso a palavra “criptografia”, provavelmente você pensa em matemática. Se, além disso, você fez uma careta, então ficará feliz em saber que não precisa se preocupar tanto com isso. *Real-World Cryptography* trata de ensinar percepções para que você ganhe uma intuição sobre como tudo funciona, e tenta evitar ao máximo as minúcias matemáticas.

Claro, eu estaria mentindo se dissesse que não há matemática envolvida na produção deste livro. Não há como ensinar criptografia sem matemática. Então, aqui está o que eu direi: ajuda se você tem um bom nível de matemática, mas se não tem, isso não deve impedi-lo de ler a maior parte deste livro. Alguns capítulos serão menos amigáveis se você não tiver uma compreensão mais avançada de matemática — especificamente os capítulos finais (14 e 15) sobre criptografia quântica e de próxima geração —, mas nada é impossível, e você pode passar por esses capítulos com força de vontade e pesquisando sobre multiplicações de matrizes e outras coisas que talvez não conheça. Se decidir pular esses, certifique-se de não pular o capítulo 16, pois ele é a cereja do bolo.

Como este livro está organizado: Um roteiro

Real-World Cryptography está dividido em duas partes. A primeira parte deve ser lida da primeira à última página e cobre a maioria dos ingredientes da criptografia: as coisas que você acabará usando como peças de Lego para construir sistemas e protocolos mais complexos.

- **Capítulo 1** é uma introdução à criptografia do mundo real, dando uma ideia do que você irá aprender.
- **Capítulo 2** fala sobre funções de hash, um algoritmo fundamental da criptografia usado para criar identificadores únicos a partir de sequências de bytes.
- **Capítulo 3** fala sobre autenticação de dados e como você pode garantir que ninguém modifique suas mensagens.
- **Capítulo 4** fala sobre criptografia, que permite a dois participantes ocultarem suas comunicações de observadores.
- **Capítulo 5** introduz as trocas de chaves, que permitem negociar um segredo comum com outra pessoa de forma interativa.
- **Capítulo 6** descreve a criptografia assimétrica, que permite que várias pessoas criptografem mensagens para uma única pessoa.
- **Capítulo 7** fala sobre assinaturas, os equivalentes criptográficos das assinaturas feitas à caneta.
- **Capítulo 8** fala sobre aleatoriedade e como gerenciar seus segredos.

A segunda parte deste livro contém os sistemas que são construídos a partir desses ingredientes.

- **Capítulo 9** ensina como criptografia e autenticação são usadas para proteger conexões entre máquinas (via o protocolo SSL/TLS).
- **Capítulo 10** descreve a criptografia de ponta a ponta, que trata de como pessoas como você e eu podem confiar umas nas outras.
- **Capítulo 11** mostra como máquinas autenticam pessoas e como as pessoas podem ajudar as máquinas a se sincronizarem umas com as outras.
- **Capítulo 12** introduz o campo nascente das criptomoedas.
- **Capítulo 13** destaca a criptografia em hardware, os dispositivos que você pode usar para evitar que suas chaves sejam extraídas.

Há dois capítulos bônus:

- o **capítulo 14** sobre criptografia pós-quântica, e
- o **capítulo 15** sobre criptografia de próxima geração.

Esses dois campos estão começando a entrar em produtos e empresas, seja porque estão se tornando mais relevantes ou porque estão ficando mais práticos e eficientes.

Embora eu não vá julgá-lo se você pular esses dois últimos capítulos, você **tem** que ler o **capítulo 16** (palavras finais) antes de colocar este livro de volta na estante. O capítulo 16 resume os diferentes desafios e lições que um praticante de criptografia (ou seja, você, depois de terminar este livro) deve ter em mente. Como disse o Tio Ben do Homem-Aranha:

“Com grandes poderes vêm grandes responsabilidades.”

Sobre o código

Este livro contém muitos exemplos de código-fonte, tanto em trechos numerados quanto incorporados ao texto comum. Em ambos os casos, o código-fonte é formatado com uma fonte de largura fixa, como esta, para separá-lo do texto comum. Às vezes, o código também aparece em **negrito** para destacar trechos que mudaram em relação a etapas anteriores no capítulo, como quando uma nova funcionalidade é adicionada a uma linha de código existente.

Em muitos casos, o código-fonte original foi reformatado; adicionamos quebras de linha e reorganizamos a indentação para acomodar o espaço disponível na página do livro. Em raros casos, mesmo isso não foi suficiente, e os trechos de código incluem marcadores de continuação de linha (↵). Além disso, comentários no código-fonte frequentemente foram removidos das listagens quando o código é descrito no texto. Anotações ao código acompanham muitas das listagens, destacando conceitos importantes.

Fórum de discussão do liveBook

A compra de *Real-World Cryptography* inclui acesso gratuito a um fórum web privado operado pela Manning Publications, onde você pode fazer comentários sobre o livro, fazer perguntas técnicas e receber ajuda do autor e de outros usuários. Para acessar o fórum, vá para:

<https://livebook.manning.com/book/real-world-cryptography/discussion>

Você também pode saber mais sobre os fóruns da Manning e sobre as regras de conduta em:

<https://livebook.manning.com/discussion>

O compromisso da Manning com seus leitores é fornecer um espaço onde um diálogo significativo entre leitores e entre leitores e o autor possa ocorrer. Isso **não é** um compromisso de participação específica por parte do autor, cuja contribuição ao fórum permanece voluntária (e não remunerada).

Sugerimos que você tente fazer ao autor algumas perguntas desafiadoras para que o interesse dele não se desvie!

O fórum e os arquivos de discussões anteriores estarão acessíveis no site da editora enquanto o livro estiver em catálogo.

Sobre o autor

DAVID WONG é engenheiro sênior de criptografia na **O(1) Labs**, trabalhando na criptomoeda **Mina**. Antes disso, ele foi o responsável pela segurança da criptomoeda **Diem** (anteriormente conhecida como **Libra**), na **Novi**, do Facebook. E antes disso, foi consultor de segurança na divisão de Serviços de Criptografia da **NCC Group**. David também é o autor deste livro, *Real-World Cryptography*.

Durante sua carreira, David participou de diversas auditorias de código aberto financiadas com recursos públicos, como **OpenSSL** e **Let's Encrypt**. Ele palestrou em várias conferências, incluindo **Black Hat** e **DEF CON**, e ministrou um curso recorrente de criptografia na Black Hat. Ele contribuiu para padrões como o **TLS 1.3** e o **Noise Protocol Framework**.

Ele encontrou vulnerabilidades em muitos sistemas, incluindo:

- CVE-2016-3959 (na biblioteca padrão do **Golang**),

- CVE-2018-12404,
- CVE-2018-19608,
- CVE-2018-16868,
- CVE-2018-16869, e
- CVE-2018-16870 (em várias bibliotecas TLS).

Entre outros feitos, ele é o autor do protocolo **Disco**:

- www.discocrypto.com
- www.embeddeddisco.com

e do projeto **DASP** (Decentralized Application Security Project) para contratos inteligentes:

- www.dasp.co

Sua pesquisa inclui:

- ataques de cache contra RSA: <http://cat.eyalro.net/>
- protocolos baseados em QUIC: <https://eprint.iacr.org/2019/028>
- ataques temporais contra ECDSA: <https://eprint.iacr.org/2015/839>
- backdoors em Diffie-Hellman: <https://eprint.iacr.org/2016/644>

Você pode vê-lo e ler sobre ele atualmente em seu blog:

www.cryptologie.net

Sobre a ilustração da capa

A figura na capa de *Real-World Cryptography* é legendada como “**Indienne de Quito**”, ou **Indiana de Quito**. A ilustração foi retirada de uma coleção de trajes de vestuário de diversos países feita por **Jacques Grasset de Saint-Sauveur (1757–1810)**, intitulada *Costumes de Differents Pays*, publicada na França em 1797. Cada ilustração é finamente desenhada e colorida à mão.

A rica variedade da coleção de Grasset de Saint-Sauveur nos lembra vividamente o quão culturalmente distintas eram as cidades e regiões do mundo há apenas 200 anos. Isoladas umas das outras, as pessoas falavam dialetos e línguas diferentes. Nas ruas ou no campo, era fácil identificar onde elas viviam e qual era seu ofício ou posição na vida apenas observando suas vestimentas.

A maneira como nos vestimos mudou desde então, e a diversidade por região — tão rica naquela época — se dissipou. Agora é difícil distinguir os habitantes de diferentes continentes, muito menos de diferentes cidades, regiões ou países. Talvez tenhamos trocado diversidade cultural por uma vida pessoal mais variada — certamente por uma vida tecnológica mais variada e acelerada.

Em uma época em que é difícil distinguir um livro de informática de outro, a Manning celebra a inventividade e a iniciativa do setor de computação com capas de livros baseadas na rica diversidade da vida regional de dois séculos atrás, trazida de volta à vida pelas ilustrações de Grasset de Saint-Sauveur.